FOIPSO Translation

FIG. 1

PRIOR ART

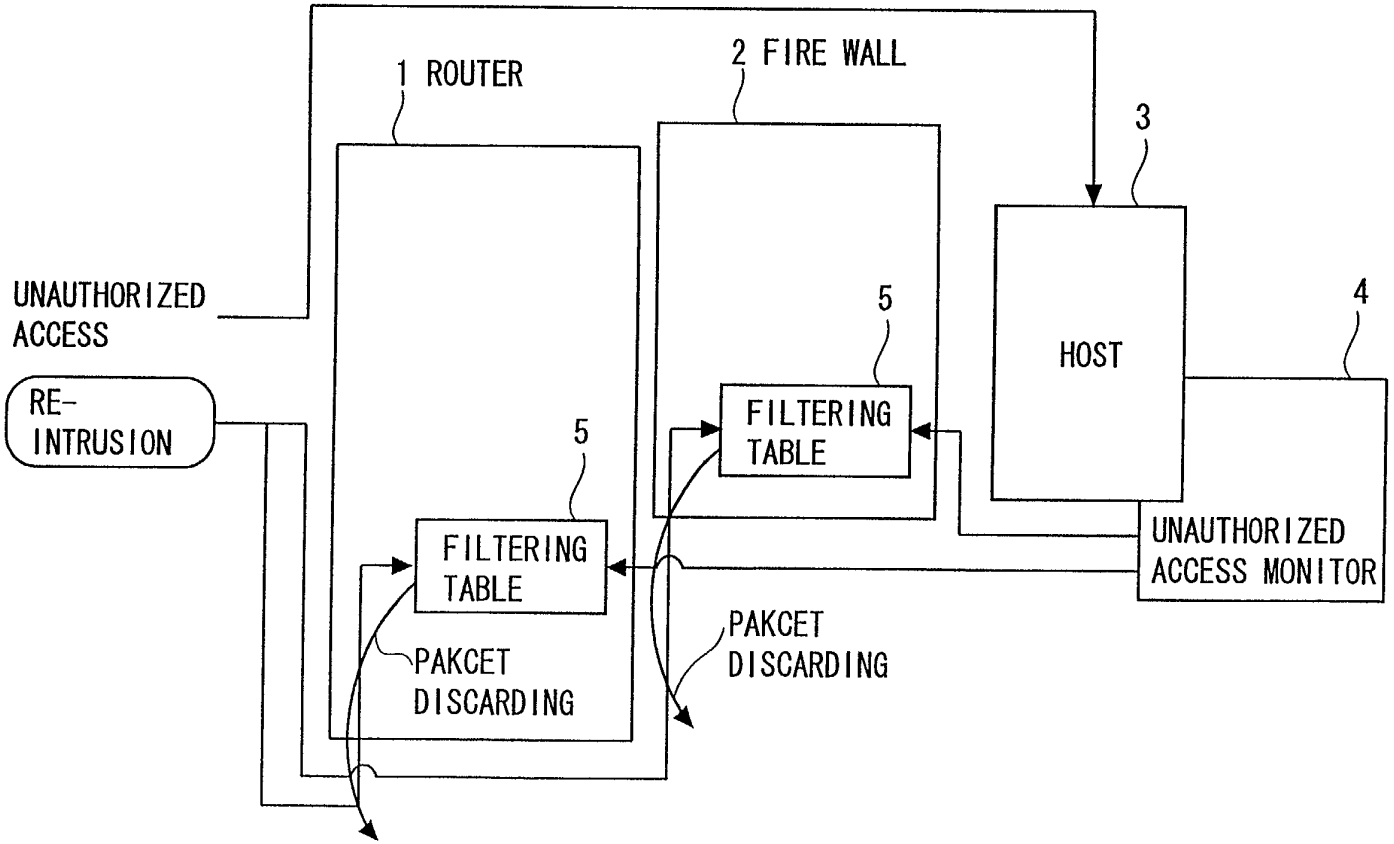


FIG. 2

PRIOR ART

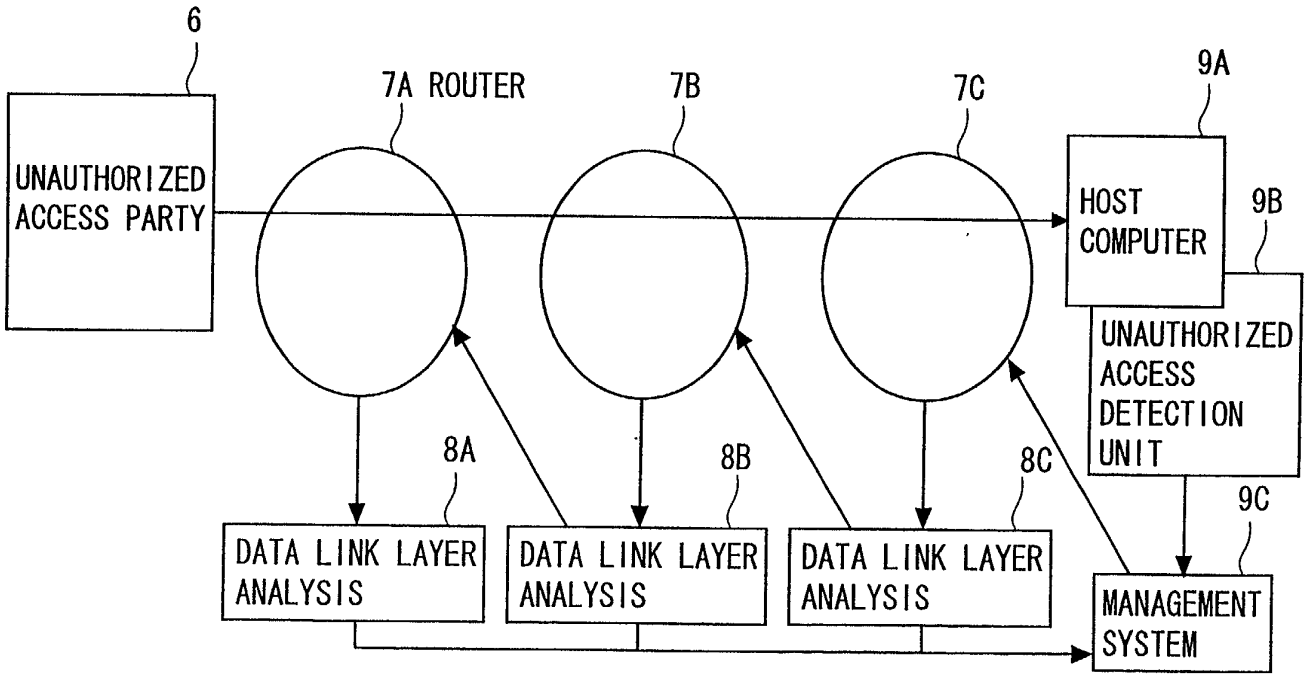


FIG. 3

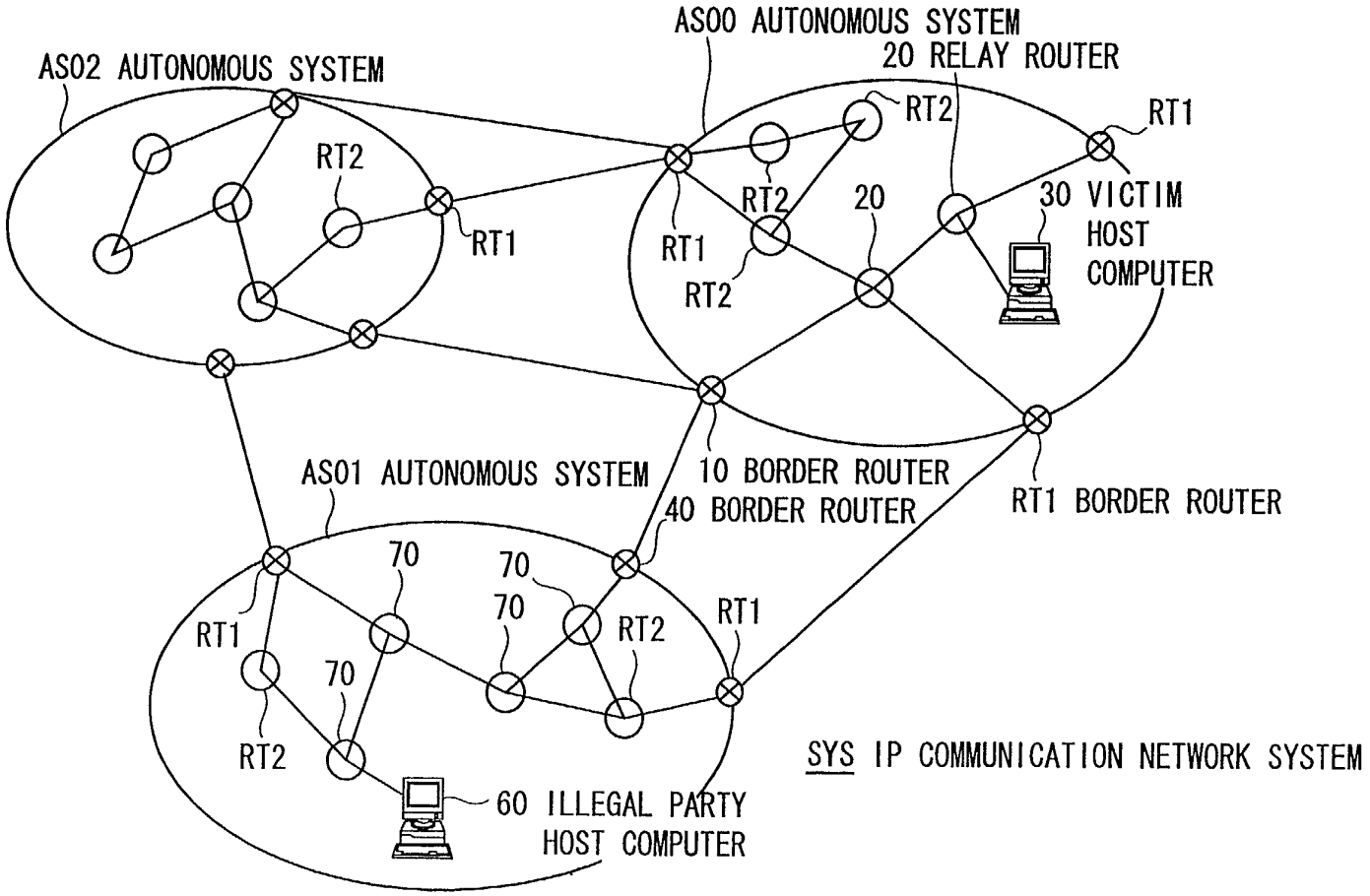

AS02 AUTONOMOUS SYSTEM
AS00 AUTONOMOUS SYSTEM
20 RELAY ROUTER
RT2
RT1
RT2
RT1
RT2
20
30 VICTIM HOST COMPUTER
RT1
RT2
AS01 AUTONOMOUS SYSTEM
10 BORDER ROUTER
40 BORDER ROUTER
RT1 BORDER ROUTER
70
70
70
70
RT1
RT2
RT1
RT2
60 ILLEGAL PARTY HOST COMPUTER
SYS IP COMMUNICATION NETWORK SYSTEM

FIG. 4

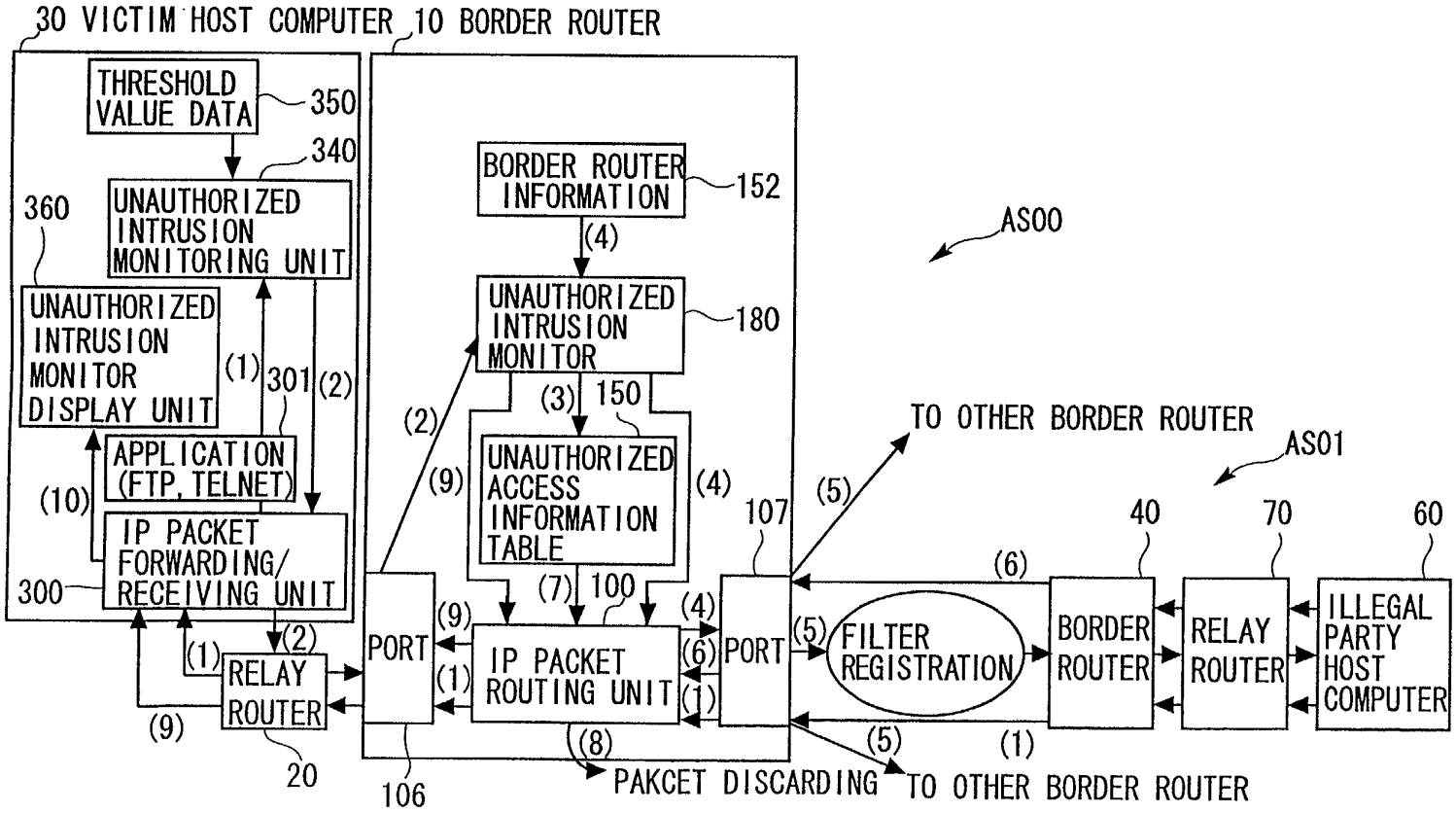

30 VICTIM HOST COMPUTER
10 BORDER ROUTER
THRESHOLD VALUE DATA
350
340
UNAUTHORIZED INTRUSION MONITORING UNIT
360
UNAUTHORIZED INTRUSION MONITOR DISPLAY UNIT
(1)
301
(2)
APPLICATION (FTP, TELNET)
(10)
IP PACKET FORWARDING/ RECEIVING UNIT
300
(1)
(2)
RELAY ROUTER
(9)
20
PORT
106
(9)
(1)
IP PACKET ROUTING UNIT
(8)
PAKCET DISCARDING
BORDER ROUTER INFORMATION
152
(4)
UNAUTHORIZED INTRUSION MONITOR
180
(3)
150
UNAUTHORIZED ACCESS INFORMATION TABLE
(7)
100
(2)
(9)
(4)
(6)
(1)
PORT
107
AS00
TO OTHER BORDER ROUTER
AS01
(5)
(6)
(5)
FILTER REGISTRATION
(5)
(1)
40
BORDER ROUTER
70
RELAY ROUTER
60
ILLEGAL PARTY HOST COMPUTER
TO OTHER BORDER ROUTER

FIG. 5

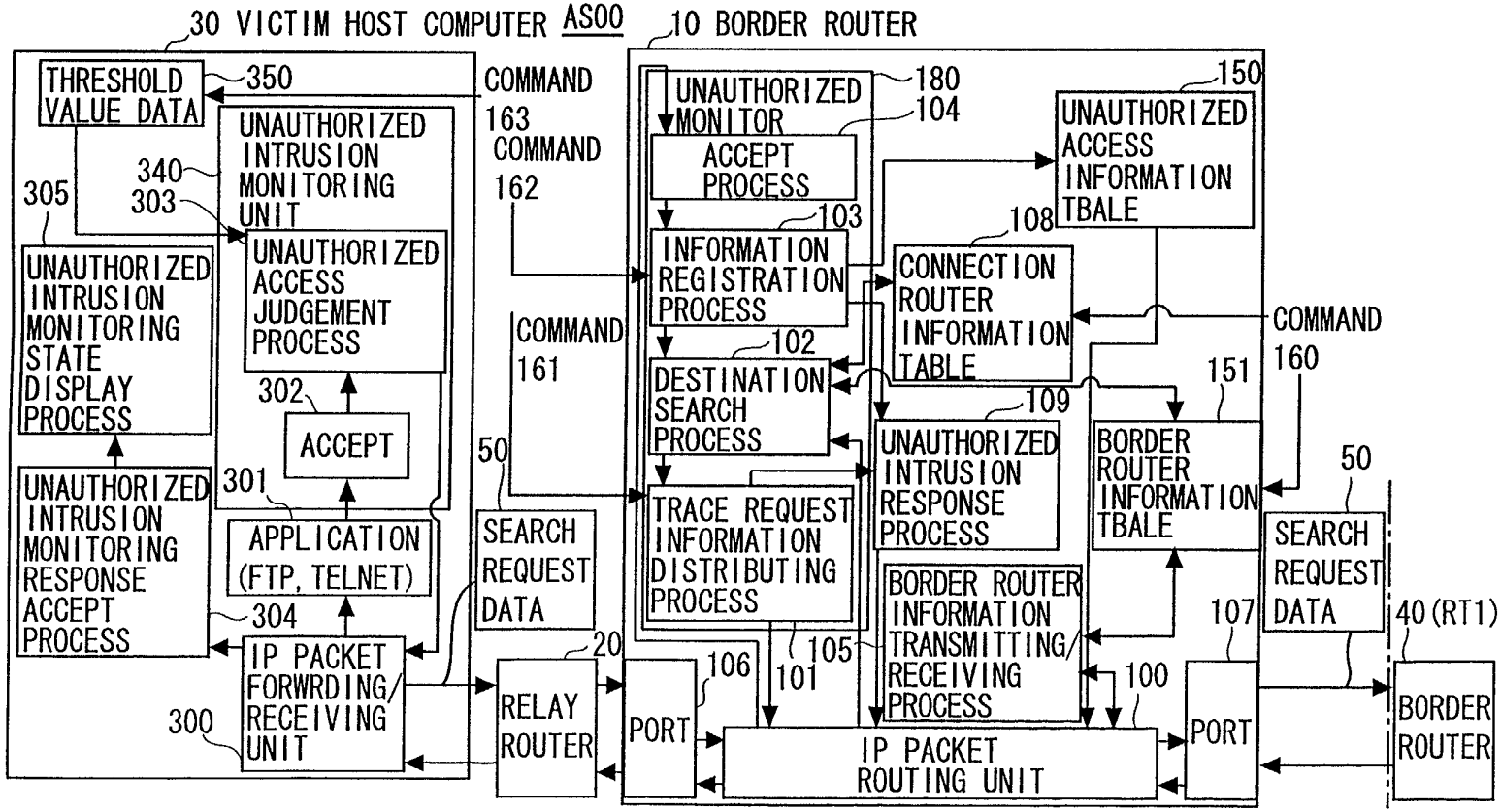

30 VICTIM HOST COMPUTER AS00
10 BORDER ROUTER
THRESHOLD VALUE DATA
350
COMMAND 163
COMMAND 162
COMMAND 161
COMMAND 160
UNAUTHORIZED INTRUSION MONITORING UNIT
340
303
305
UNAUTHORIZED INTRUSION MONITORING STATE DISPLAY PROCESS
UNAUTHORIZED ACCESS JUDGEMENT PROCESS
302
ACCEPT
301
APPLICATION (FTP, TELNET)
UNAUTHORIZED INTRUSION MONITORING RESPONSE ACCEPT PROCESS
304
IP PACKET FORWRDING/ RECEIVING UNIT
300
SEARCH REQUEST DATA
50
RELAY ROUTER
20
PORT
106
IP PACKET ROUTING UNIT
101
UNAUTHORIZED MONITOR
180
ACCEPT PROCESS
104
INFORMATION REGISTRATION PROCESS
103
DESTINATION SEARCH PROCESS
102
TRACE REQUEST INFORMATION DISTRIBUTING PROCESS
UNAUTHORIZED ACCESS INFORMATION TBALE
150
CONNECTION ROUTER INFORMATION TABLE
108
UNAUTHORIZED INTRUSION RESPONSE PROCESS
109
BORDER ROUTER INFORMATION TRANSMITTING/ RECEIVING PROCESS
105
100
BORDER ROUTER INFORMATION TBALE
151
SEARCH REQUEST DATA
50
107
PORT
40 (RT1)
BORDER ROUTER

FIG. 6

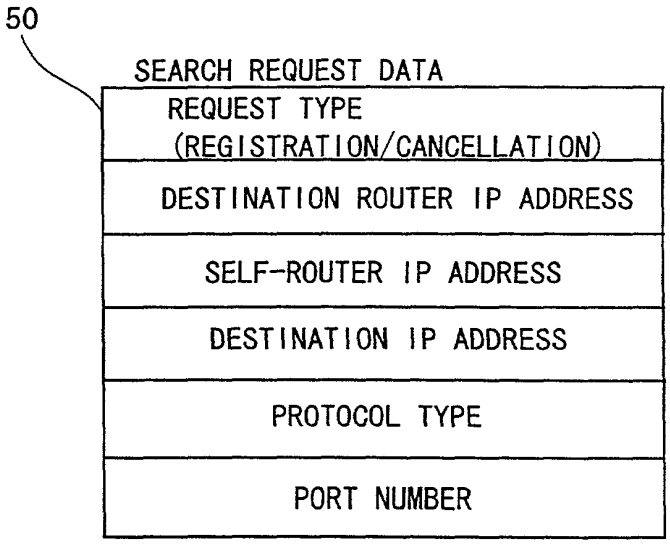

50
SEARCH REQUEST DATA
REQUEST TYPE (REGISTRATION/CANCELLATION)
DESTINATION ROUTER IP ADDRESS
SELF-ROUTER IP ADDRESS
DESTINATION IP ADDRESS
PROTOCOL TYPE
PORT NUMBER

FIG. 7

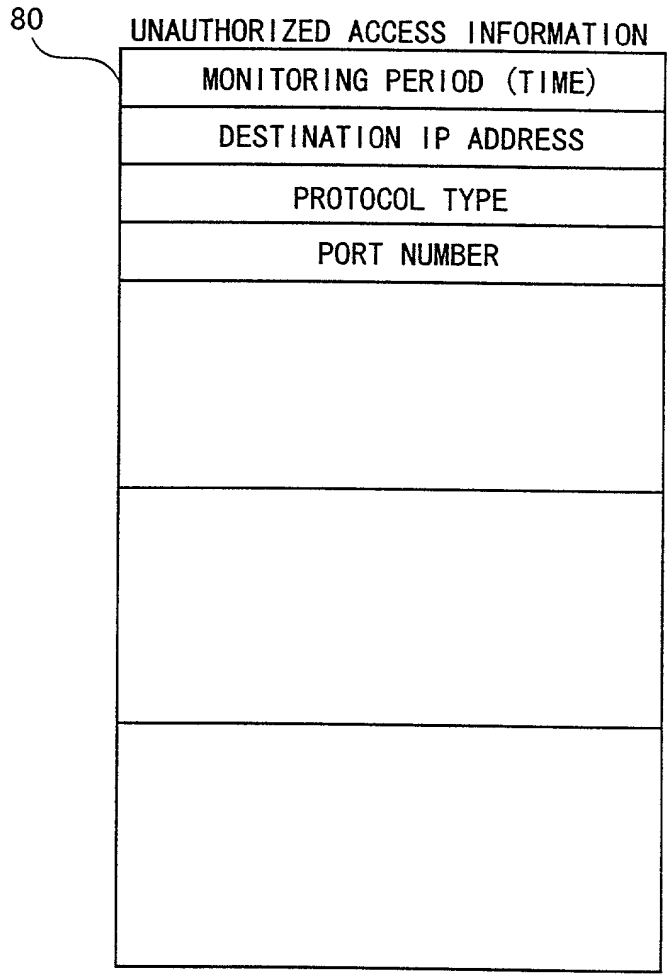

80
UNAUTHORIZED ACCESS INFORMATION
MONITORING PERIOD (TIME)
DESTINATION IP ADDRESS
PROTOCOL TYPE
PORT NUMBER

FIG. 8

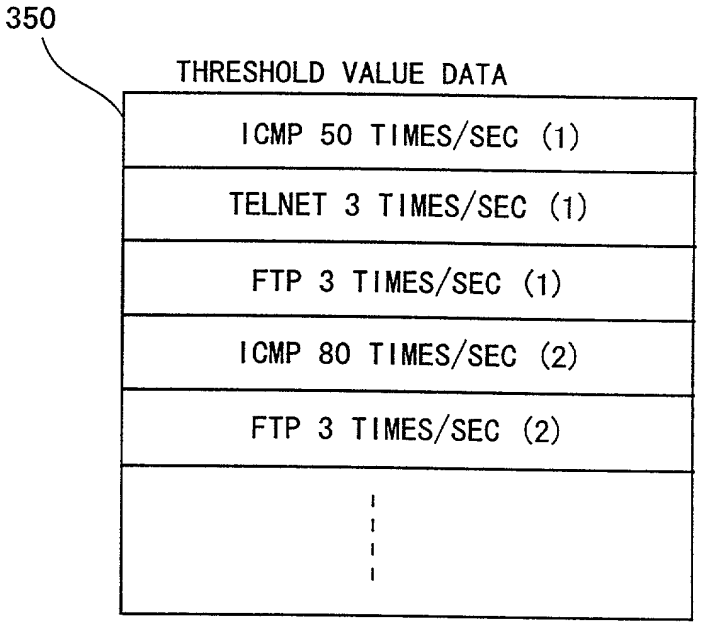

350
THRESHOLD VALUE DATA
ICMP 50 TIMES/SEC (1)
TELNET 3 TIMES/SEC (1)
FTP 3 TIMES/SEC (1)
ICMP 80 TIMES/SEC (2)
FTP 3 TIMES/SEC (2)

FIG. 9

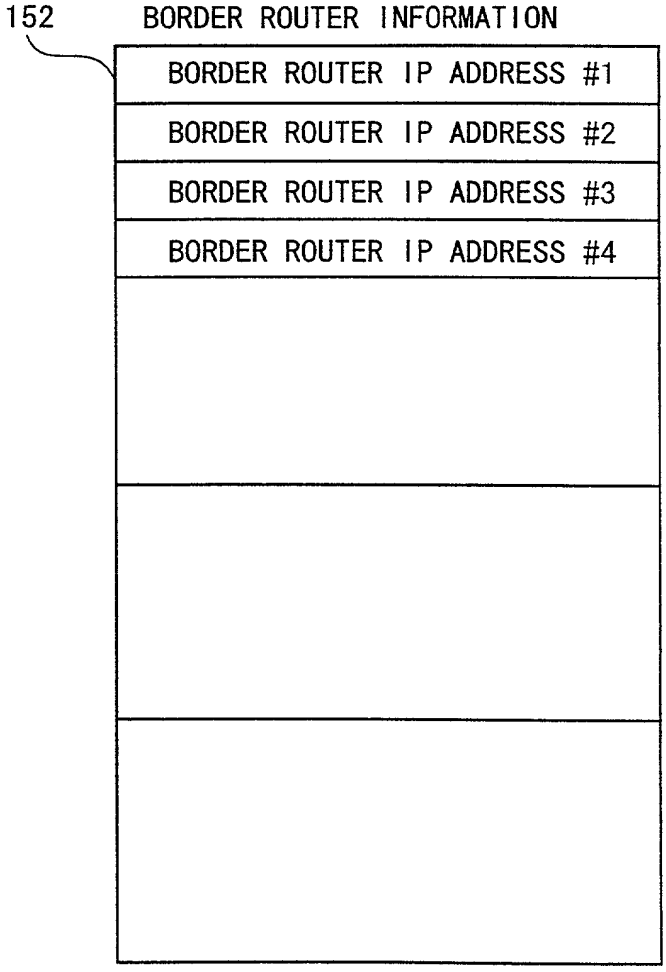

152
BORDER ROUTER INFORMATION
BORDER ROUTER IP ADDRESS #1
BORDER ROUTER IP ADDRESS #2
BORDER ROUTER IP ADDRESS #3
BORDER ROUTER IP ADDRESS #4

FIG. 10

90

CONNECTION ROUTER INFORMATION

SELF-ROUTER INFORMATION	CONNECTION ROUTER INFORMATION
MAC ADDRESS #1	CONNECTION ROUTER IP ADDRESS #1
VPI/VCI#1	CONNECTION ROUTER IP ADDRESS #2
INPUT PORT INFORMATION #1	CONNECTION ROUTER IP ADDRESS #3
⋮	⋮

FIG. 11

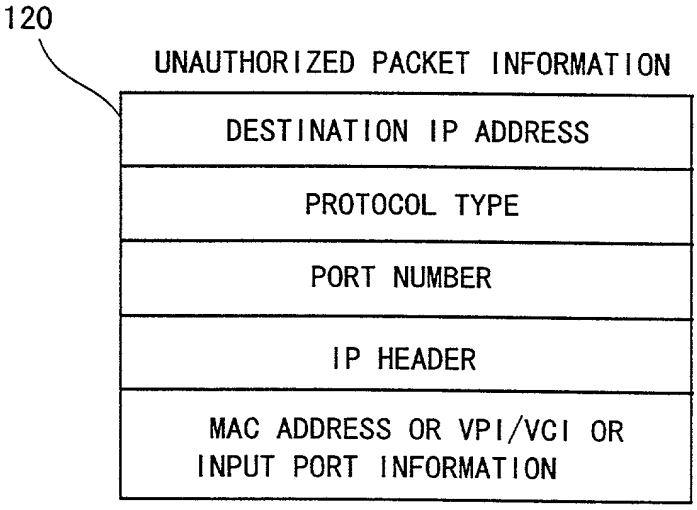

120
UNAUTHORIZED PACKET INFORMATION
DESTINATION IP ADDRESS
PROTOCOL TYPE
PORT NUMBER
IP HEADER
MAC ADDRESS OR VPI/VCI OR
INPUT PORT INFORMATION

FIG. 12

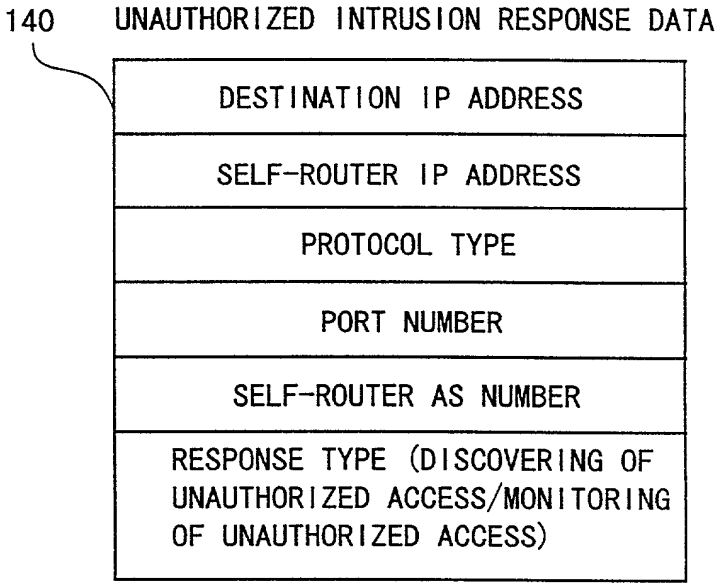

140
UNAUTHORIZED INTRUSION RESPONSE DATA
DESTINATION IP ADDRESS
SELF-ROUTER IP ADDRESS
PROTOCOL TYPE
PORT NUMBER
SELF-ROUTER AS NUMBER
RESPONSE TYPE (DISCOVERING OF UNAUTHORIZED ACCESS/MONITORING OF UNAUTHORIZED ACCESS)

FIG. 13

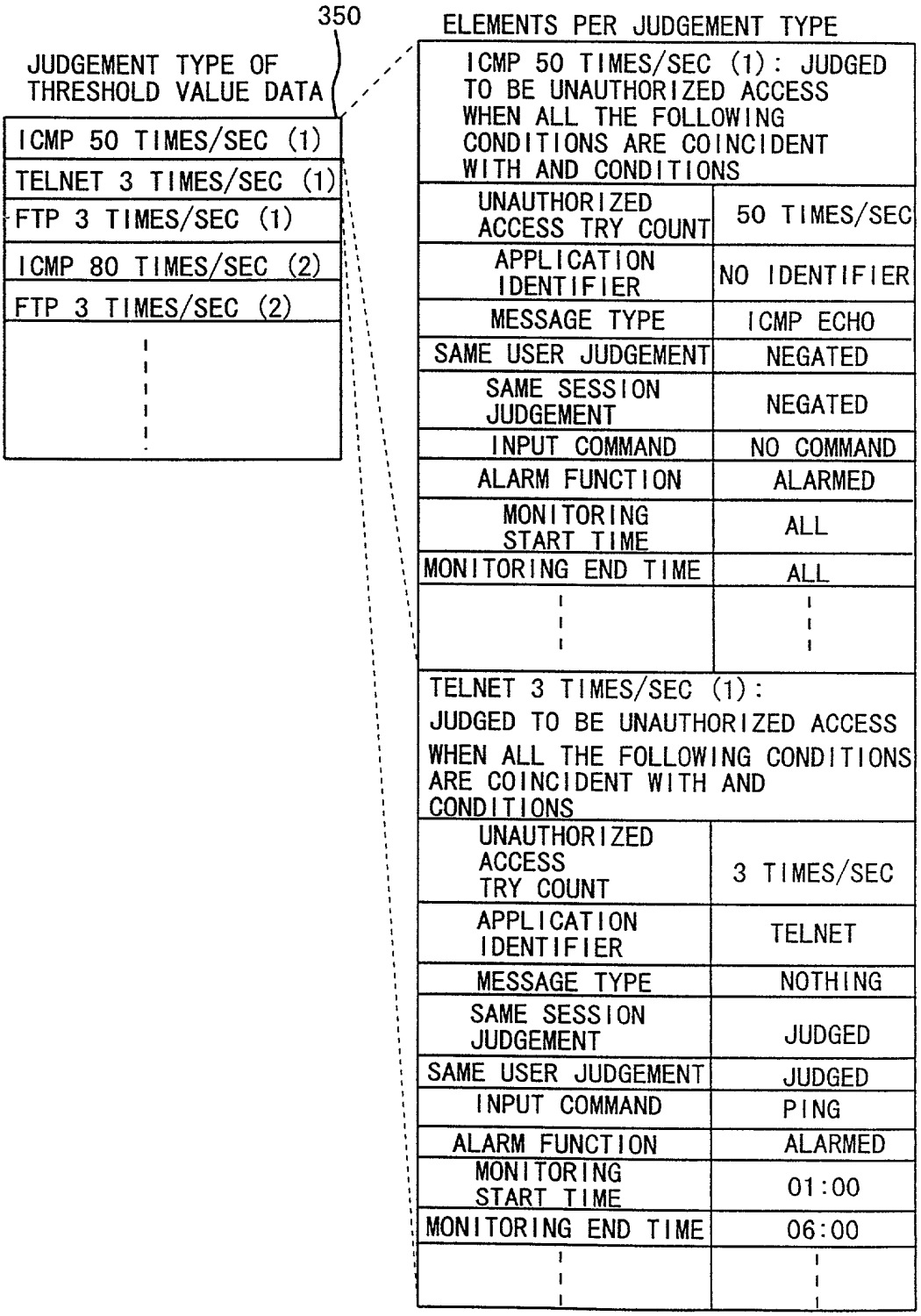
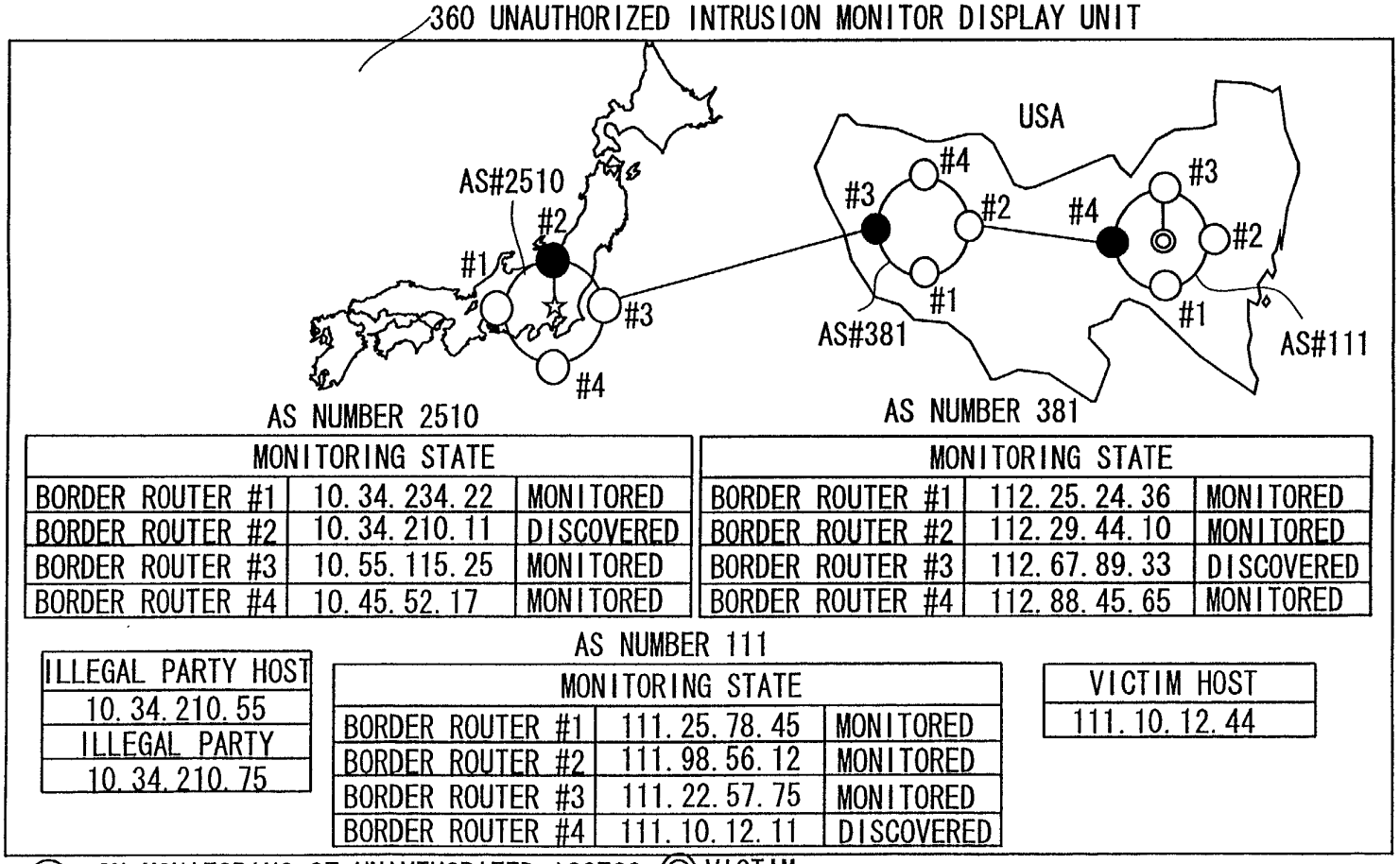

350
JUDGEMENT TYPE OF THRESHOLD VALUE DATA
ICMP 50 TIMES/SEC (1)
TELNET 3 TIMES/SEC (1)
FTP 3 TIMES/SEC (1)
ICMP 80 TIMES/SEC (2)
FTP 3 TIMES/SEC (2)
ELEMENTS PER JUDGEMENT TYPE
ICMP 50 TIMES/SEC (1): JUDGED TO BE UNAUTHORIZED ACCESS WHEN ALL THE FOLLOWING CONDITIONS ARE COINCIDENT WITH AND CONDITIONS
UNAUTHORIZED ACCESS TRY COUNT
50 TIMES/SEC
APPLICATION IDENTIFIER
NO IDENTIFIER
MESSAGE TYPE
ICMP ECHO
SAME USER JUDGEMENT
NEGATED
SAME SESSION JUDGEMENT
NEGATED
INPUT COMMAND
NO COMMAND
ALARM FUNCTION
ALARMED
MONITORING START TIME
ALL
MONITORING END TIME
ALL
TELNET 3 TIMES/SEC (1): JUDGED TO BE UNAUTHORIZED ACCESS WHEN ALL THE FOLLOWING CONDITIONS ARE COINCIDENT WITH AND CONDITIONS
UNAUTHORIZED ACCESS TRY COUNT
3 TIMES/SEC
APPLICATION IDENTIFIER
TELNET
MESSAGE TYPE
NOTHING
SAME SESSION JUDGEMENT
JUDGED
SAME USER JUDGEMENT
JUDGED
INPUT COMMAND
PING
ALARM FUNCTION
ALARMED
MONITORING START TIME
01:00
MONITORING END TIME
06:00

FIG. 14



MONITORING STATE		
BORDER ROUTER #1	10.34.234.22	MONITORED
BORDER ROUTER #2	10.34.210.11	DISCOVERED
BORDER ROUTER #3	10.55.115.25	MONITORED
BORDER ROUTER #4	10.45.52.17	MONITORED

MONITORING STATE		
BORDER ROUTER #1	112.25.24.36	MONITORED
BORDER ROUTER #2	112.29.44.10	MONITORED
BORDER ROUTER #3	112.67.89.33	DISCOVERED
BORDER ROUTER #4	112.88.45.65	MONITORED

ILLEGAL PARTY HOST
10.34.210.55
ILLEGAL PARTY
10.34.210.75

MONITORING STATE		
BORDER ROUTER #1	111.25.78.45	MONITORED
BORDER ROUTER #2	111.98.56.12	MONITORED
BORDER ROUTER #3	111.22.57.75	MONITORED
BORDER ROUTER #4	111.10.12.11	DISCOVERED

VICTIM HOST
111.10.12.44

FIG. 15

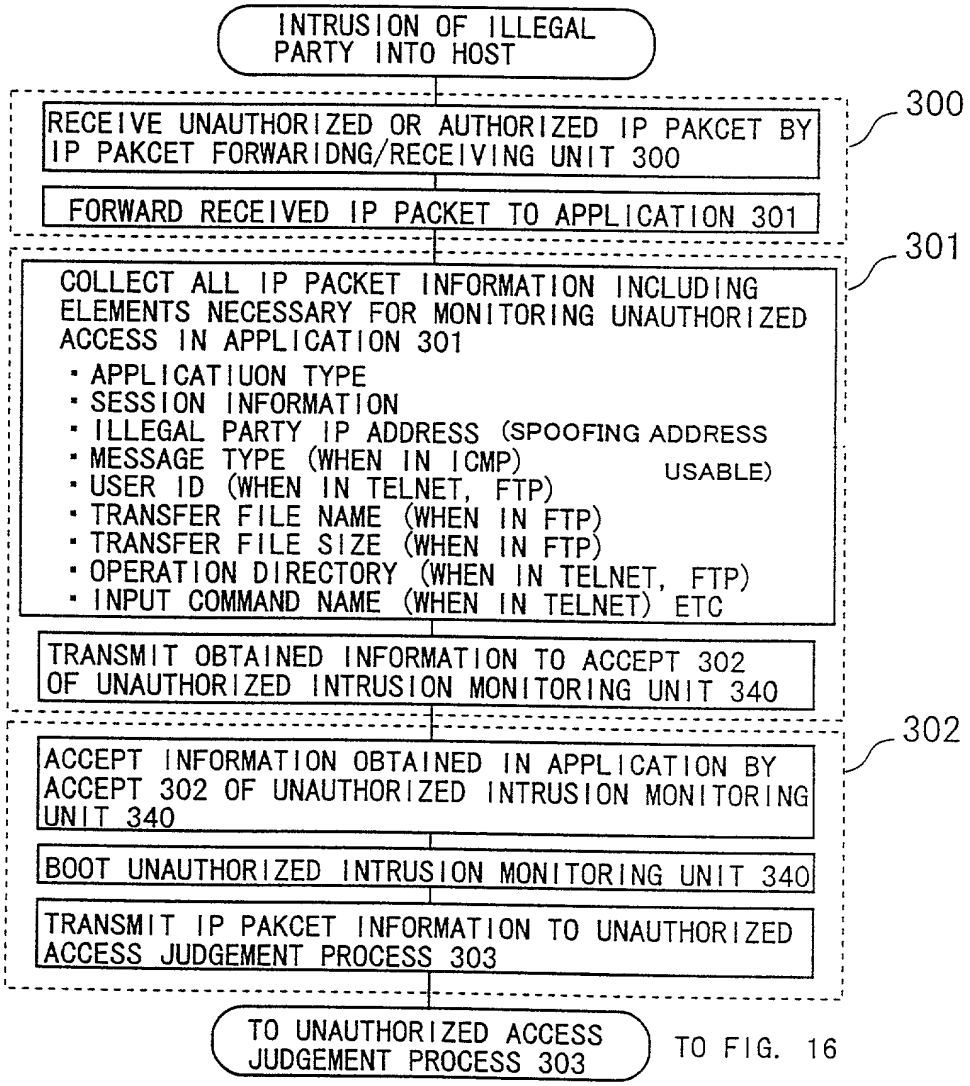

INTRUSION OF ILLEGAL PARTY INTO HOST
RECEIVE UNAUTHORIZED OR AUTHORIZED IP PAKCET BY IP PAKCET FORWARIDNG/RECEIVING UNIT 300
300
FORWARD RECEIVED IP PACKET TO APPLICATION 301
301
COLLECT ALL IP PACKET INFORMATION INCLUDING ELEMENTS NECESSARY FOR MONITORING UNAUTHORIZED ACCESS IN APPLICATION 301
• APPLICATIUON TYPE
• SESSION INFORMATION
• ILLEGAL PARTY IP ADDRESS (SPOOFING ADDRESS USABLE)
• MESSAGE TYPE (WHEN IN ICMP)
• USER ID (WHEN IN TELNET, FTP)
• TRANSFER FILE NAME (WHEN IN FTP)
• TRANSFER FILE SIZE (WHEN IN FTP)
• OPERATION DIRECTORY (WHEN IN TELNET, FTP)
• INPUT COMMAND NAME (WHEN IN TELNET) ETC
TRANSMIT OBTAINED INFORMATION TO ACCEPT 302 OF UNAUTHORIZED INTRUSION MONITORING UNIT 340
302
ACCEPT INFORMATION OBTAINED IN APPLICATION BY ACCEPT 302 OF UNAUTHORIZED INTRUSION MONITORING UNIT 340
BOOT UNAUTHORIZED INTRUSION MONITORING UNIT 340
TRANSMIT IP PAKCET INFORMATION TO UNAUTHORIZED ACCESS JUDGEMENT PROCESS 303
TO UNAUTHORIZED ACCESS JUDGEMENT PROCESS 303
TO FIG. 16

FIG. 16

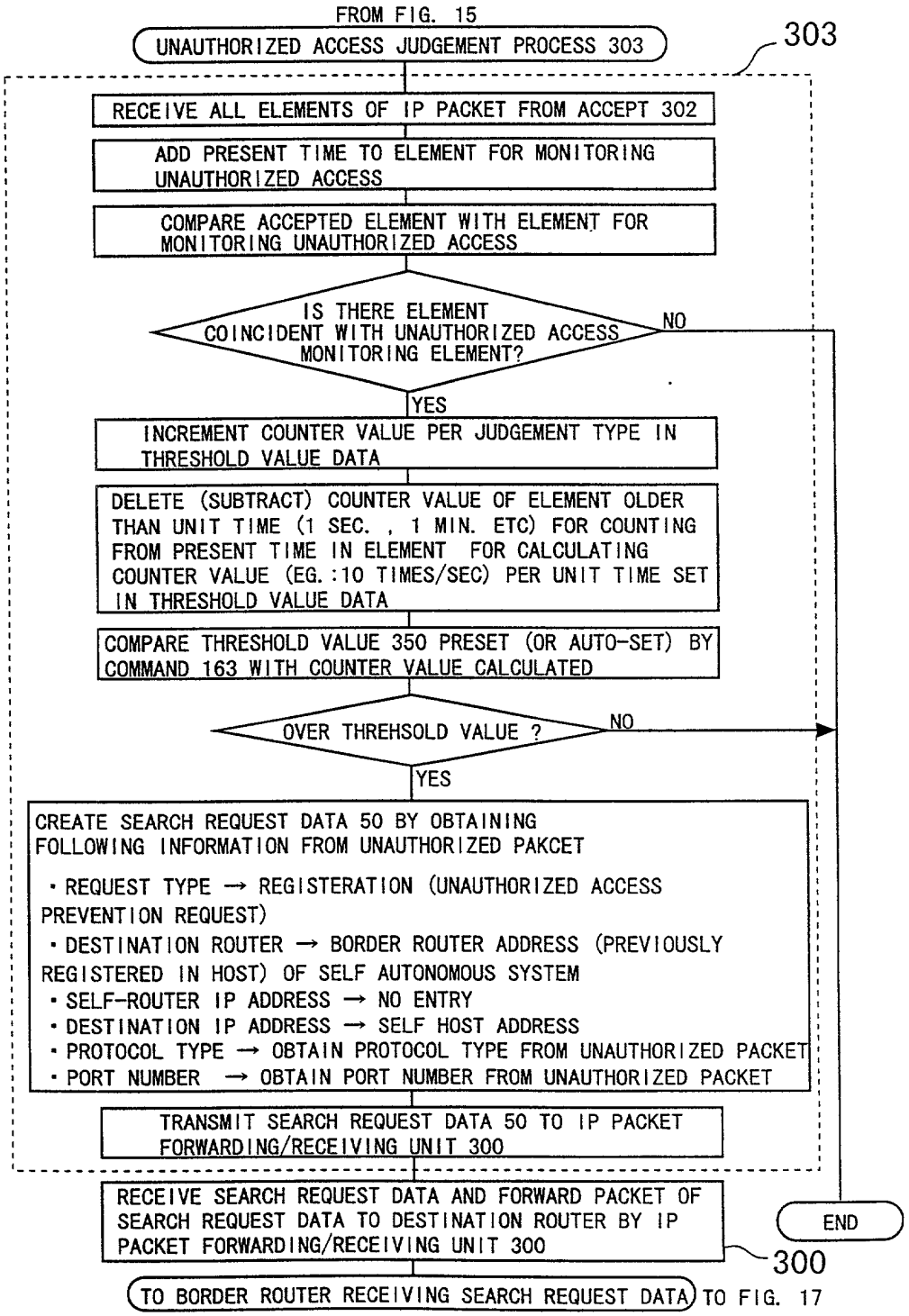

FROM FIG. 15
UNAUTHORIZED ACCESS JUDGEMENT PROCESS 303
303
RECEIVE ALL ELEMENTS OF IP PACKET FROM ACCEPT 302
ADD PRESENT TIME TO ELEMENT FOR MONITORING UNAUTHORIZED ACCESS
COMPARE ACCEPTED ELEMENT WITH ELEMENT FOR MONITORING UNAUTHORIZED ACCESS
IS THERE ELEMENT COINCIDENT WITH UNAUTHORIZED ACCESS MONITORING ELEMENT?
NO
YES
INCREMENT COUNTER VALUE PER JUDGEMENT TYPE IN THRESHOLD VALUE DATA
DELETE (SUBTRACT) COUNTER VALUE OF ELEMENT OLDER THAN UNIT TIME (1 SEC. , 1 MIN. ETC) FOR COUNTING FROM PRESENT TIME IN ELEMENT FOR CALCULATING COUNTER VALUE (EG.:10 TIMES/SEC) PER UNIT TIME SET IN THRESHOLD VALUE DATA
COMPARE THRESHOLD VALUE 350 PRESET (OR AUTO-SET) BY COMMAND 163 WITH COUNTER VALUE CALCULATED
OVER THREHSOLD VALUE ?
NO
YES
CREATE SEARCH REQUEST DATA 50 BY OBTAINING FOLLOWING INFORMATION FROM UNAUTHORIZED PAKCET
• REQUEST TYPE → REGISTERATION (UNAUTHORIZED ACCESS PREVENTION REQUEST)
• DESTINATION ROUTER → BORDER ROUTER ADDRESS (PREVIOUSLY REGISTERED IN HOST) OF SELF AUTONOMOUS SYSTEM
• SELF-ROUTER IP ADDRESS → NO ENTRY
• DESTINATION IP ADDRESS → SELF HOST ADDRESS
• PROTOCOL TYPE → OBTAIN PROTOCOL TYPE FROM UNAUTHORIZED PACKET
• PORT NUMBER → OBTAIN PORT NUMBER FROM UNAUTHORIZED PACKET
TRANSMIT SEARCH REQUEST DATA 50 TO IP PACKET FORWARDING/RECEIVING UNIT 300
RECEIVE SEARCH REQUEST DATA AND FORWARD PACKET OF SEARCH REQUEST DATA TO DESTINATION ROUTER BY IP PACKET FORWARDING/RECEIVING UNIT 300
300
END
TO BORDER ROUTER RECEIVING SEARCH REQUEST DATA
TO FIG. 17

FIG. 17

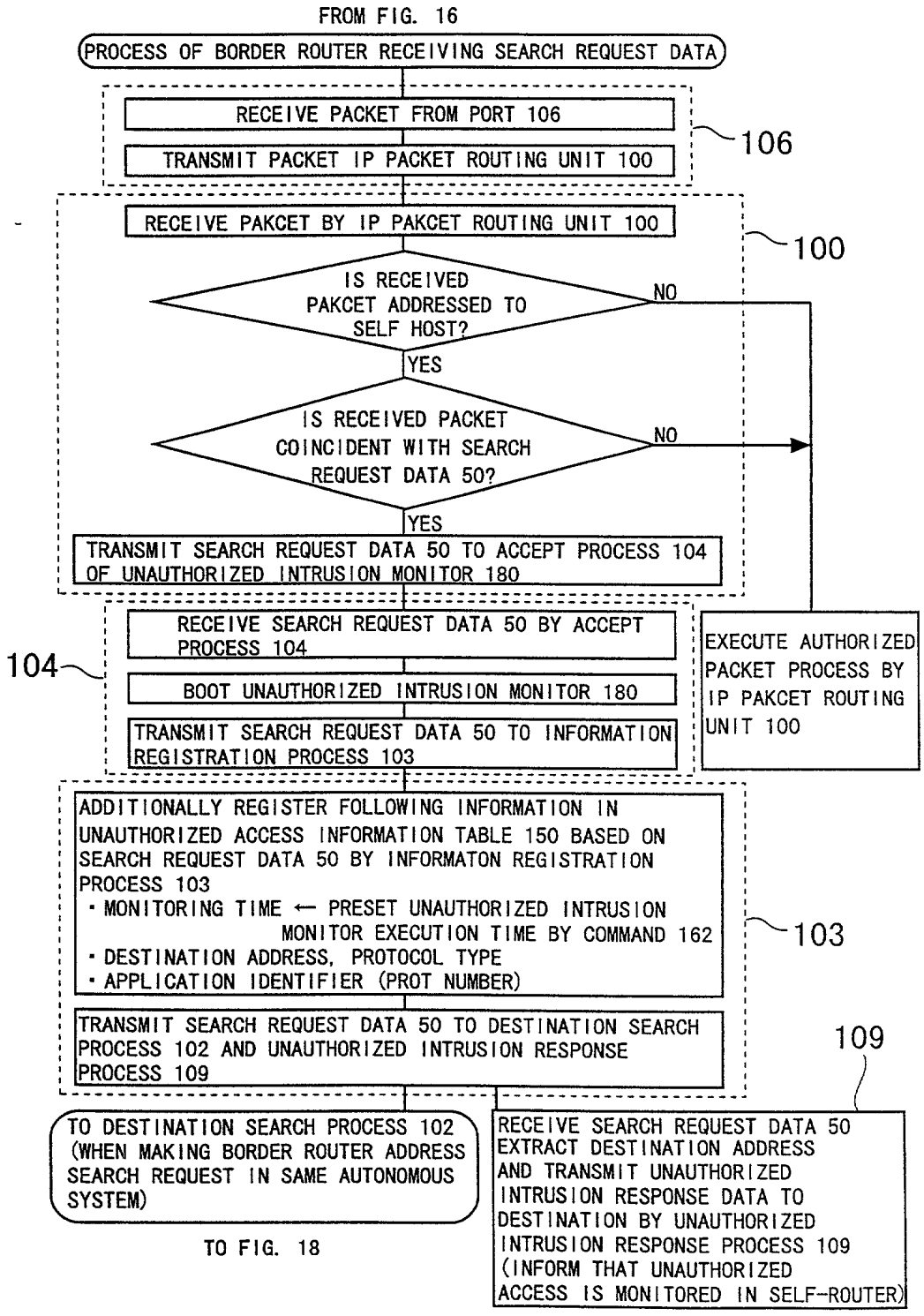

FROM FIG. 16
PROCESS OF BORDER ROUTER RECEIVING SEARCH REQUEST DATA
RECEIVE PACKET FROM PORT 106
TRANSMIT PACKET IP PACKET ROUTING UNIT 100
106
RECEIVE PAKCET BY IP PAKCET ROUTING UNIT 100
100
IS RECEIVED PAKCET ADDRESSED TO SELF HOST?
NO
YES
IS RECEIVED PACKET COINCIDENT WITH SEARCH REQUEST DATA 50?
NO
YES
TRANSMIT SEARCH REQUEST DATA 50 TO ACCEPT PROCESS 104 OF UNAUTHORIZED INTRUSION MONITOR 180
104
RECEIVE SEARCH REQUEST DATA 50 BY ACCEPT PROCESS 104
BOOT UNAUTHORIZED INTRUSION MONITOR 180
TRANSMIT SEARCH REQUEST DATA 50 TO INFORMATION REGISTRATION PROCESS 103
EXECUTE AUTHORIZED PACKET PROCESS BY IP PAKCET ROUTING UNIT 100
ADDITIONALLY REGISTER FOLLOWING INFORMATION IN UNAUTHORIZED ACCESS INFORMATION TABLE 150 BASED ON SEARCH REQUEST DATA 50 BY INFORMATON REGISTRATION PROCESS 103
・MONITORING TIME ← PRESET UNAUTHORIZED INTRUSION MONITOR EXECUTION TIME BY COMMAND 162
・DESTINATION ADDRESS, PROTOCOL TYPE
・APPLICATION IDENTIFIER (PROT NUMBER)
103
TRANSMIT SEARCH REQUEST DATA 50 TO DESTINATION SEARCH PROCESS 102 AND UNAUTHORIZED INTRUSION RESPONSE PROCESS 109
109
TO DESTINATION SEARCH PROCESS 102 (WHEN MAKING BORDER ROUTER ADDRESS SEARCH REQUEST IN SAME AUTONOMOUS SYSTEM)
RECEIVE SEARCH REQUEST DATA 50 EXTRACT DESTINATION ADDRESS AND TRANSMIT UNAUTHORIZED INTRUSION RESPONSE DATA TO DESTINATION BY UNAUTHORIZED INTRUSION RESPONSE PROCESS 109 (INFORM THAT UNAUTHORIZED ACCESS IS MONITORED IN SELF-ROUTER)
TO FIG. 18

FIG. 18

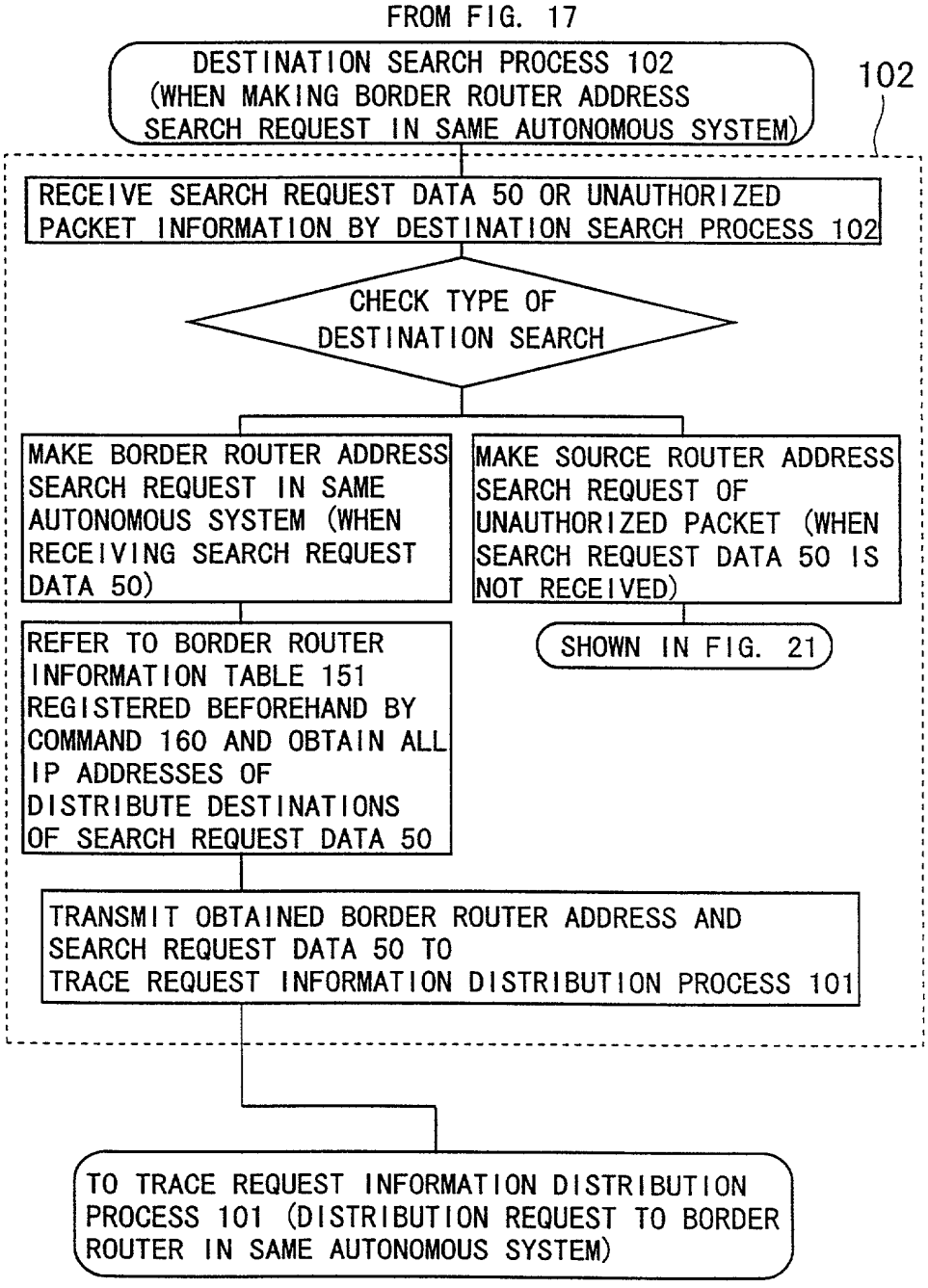

FROM FIG. 17
DESTINATION SEARCH PROCESS 102 (WHEN MAKING BORDER ROUTER ADDRESS SEARCH REQUEST IN SAME AUTONOMOUS SYSTEM)
102
RECEIVE SEARCH REQUEST DATA 50 OR UNAUTHORIZED PACKET INFORMATION BY DESTINATION SEARCH PROCESS 102
CHECK TYPE OF DESTINATION SEARCH
MAKE BORDER ROUTER ADDRESS SEARCH REQUEST IN SAME AUTONOMOUS SYSTEM (WHEN RECEIVING SEARCH REQUEST DATA 50)
MAKE SOURCE ROUTER ADDRESS SEARCH REQUEST OF UNAUTHORIZED PACKET (WHEN SEARCH REQUEST DATA 50 IS NOT RECEIVED)
SHOWN IN FIG. 21
REFER TO BORDER ROUTER INFORMATION TABLE 151 REGISTERED BEFOREHAND BY COMMAND 160 AND OBTAIN ALL IP ADDRESSES OF DISTRIBUTE DESTINATIONS OF SEARCH REQUEST DATA 50
TRANSMIT OBTAINED BORDER ROUTER ADDRESS AND SEARCH REQUEST DATA 50 TO TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101
TO TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101 (DISTRIBUTION REQUEST TO BORDER ROUTER IN SAME AUTONOMOUS SYSTEM)
TO FIG. 19

FIG. 19

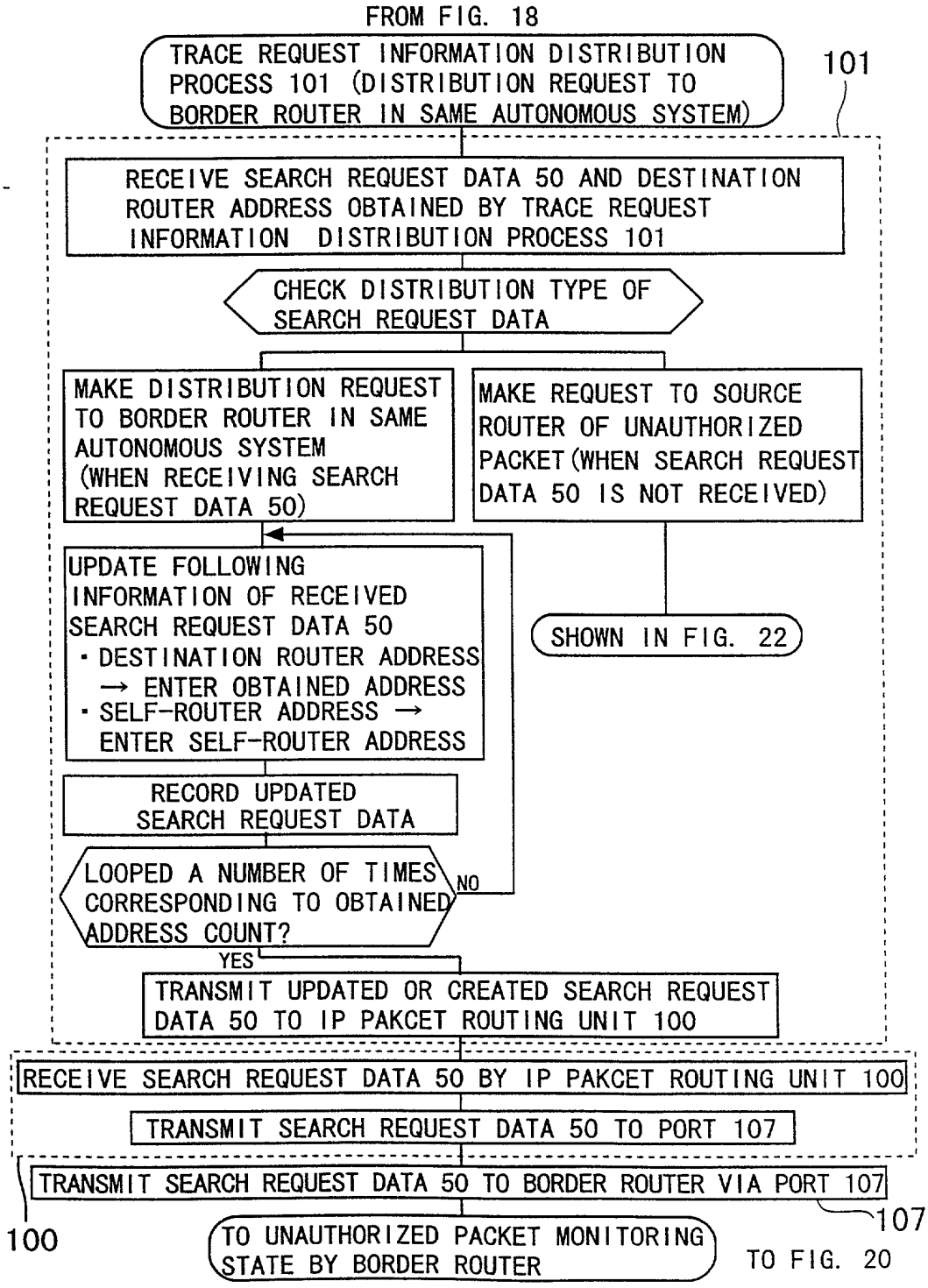

FROM FIG. 18
TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101 (DISTRIBUTION REQUEST TO BORDER ROUTER IN SAME AUTONOMOUS SYSTEM)
101
RECEIVE SEARCH REQUEST DATA 50 AND DESTINATION ROUTER ADDRESS OBTAINED BY TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101
CHECK DISTRIBUTION TYPE OF SEARCH REQUEST DATA
MAKE DISTRIBUTION REQUEST TO BORDER ROUTER IN SAME AUTONOMOUS SYSTEM (WHEN RECEIVING SEARCH REQUEST DATA 50)
MAKE REQUEST TO SOURCE ROUTER OF UNAUTHORIZED PACKET (WHEN SEARCH REQUEST DATA 50 IS NOT RECEIVED)
UPDATE FOLLOWING INFORMATION OF RECEIVED SEARCH REQUEST DATA 50
・DESTINATION ROUTER ADDRESS → ENTER OBTAINED ADDRESS
・SELF-ROUTER ADDRESS → ENTER SELF-ROUTER ADDRESS
SHOWN IN FIG. 22
RECORD UPDATED SEARCH REQUEST DATA
LOOPED A NUMBER OF TIMES CORRESPONDING TO OBTAINED ADDRESS COUNT?
NO
YES
TRANSMIT UPDATED OR CREATED SEARCH REQUEST DATA 50 TO IP PAKCET ROUTING UNIT 100
RECEIVE SEARCH REQUEST DATA 50 BY IP PAKCET ROUTING UNIT 100
TRANSMIT SEARCH REQUEST DATA 50 TO PORT 107
TRANSMIT SEARCH REQUEST DATA 50 TO BORDER ROUTER VIA PORT 107
107
100
TO UNAUTHORIZED PACKET MONITORING STATE BY BORDER ROUTER
TO FIG. 20

FIG. 20

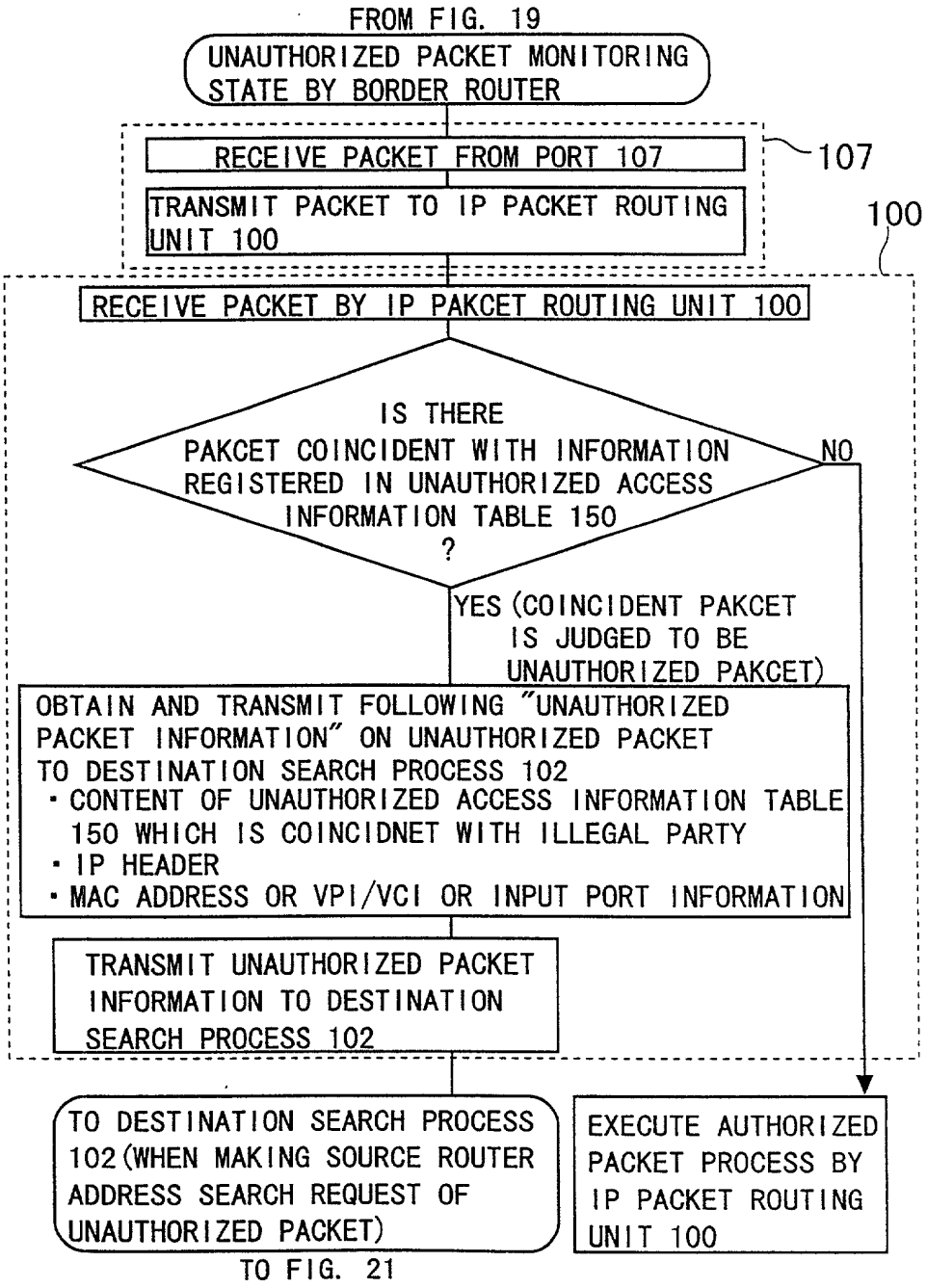
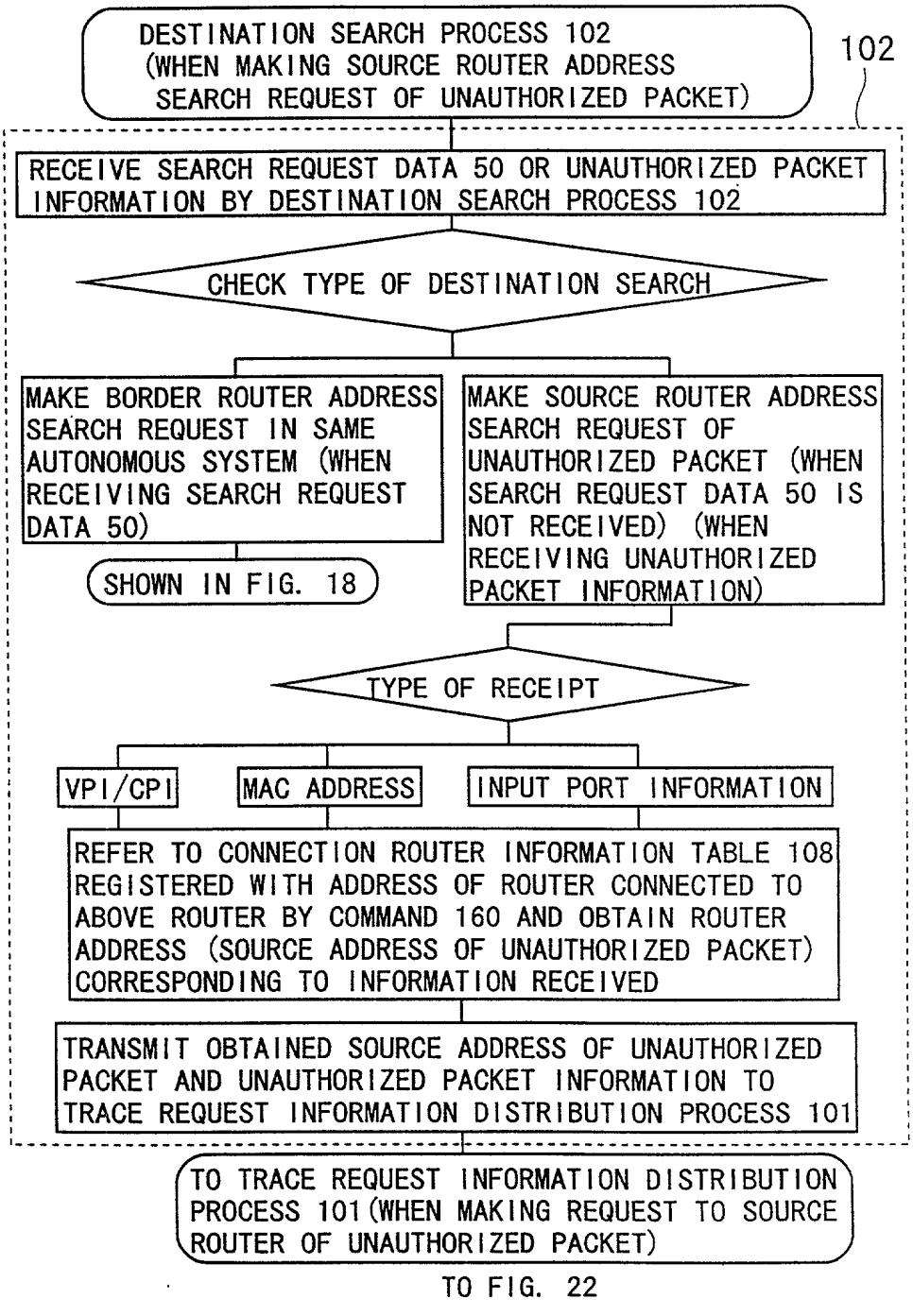

FROM FIG. 19
UNAUTHORIZED PACKET MONITORING STATE BY BORDER ROUTER
RECEIVE PACKET FROM PORT 107
107
TRANSMIT PACKET TO IP PACKET ROUTING UNIT 100
100
RECEIVE PACKET BY IP PAKCET ROUTING UNIT 100
IS THERE PAKCET COINCIDENT WITH INFORMATION REGISTERED IN UNAUTHORIZED ACCESS INFORMATION TABLE 150 ?
NO
YES (COINCIDENT PAKCET IS JUDGED TO BE UNAUTHORIZED PAKCET)
OBTAIN AND TRANSMIT FOLLOWING "UNAUTHORIZED PACKET INFORMATION" ON UNAUTHORIZED PACKET TO DESTINATION SEARCH PROCESS 102
・CONTENT OF UNAUTHORIZED ACCESS INFORMATION TABLE 150 WHICH IS COINCIDNET WITH ILLEGAL PARTY
・IP HEADER
・MAC ADDRESS OR VPI/VCI OR INPUT PORT INFORMATION
TRANSMIT UNAUTHORIZED PACKET INFORMATION TO DESTINATION SEARCH PROCESS 102
TO DESTINATION SEARCH PROCESS 102 (WHEN MAKING SOURCE ROUTER ADDRESS SEARCH REQUEST OF UNAUTHORIZED PACKET)
EXECUTE AUTHORIZED PACKET PROCESS BY IP PACKET ROUTING UNIT 100
TO FIG. 21

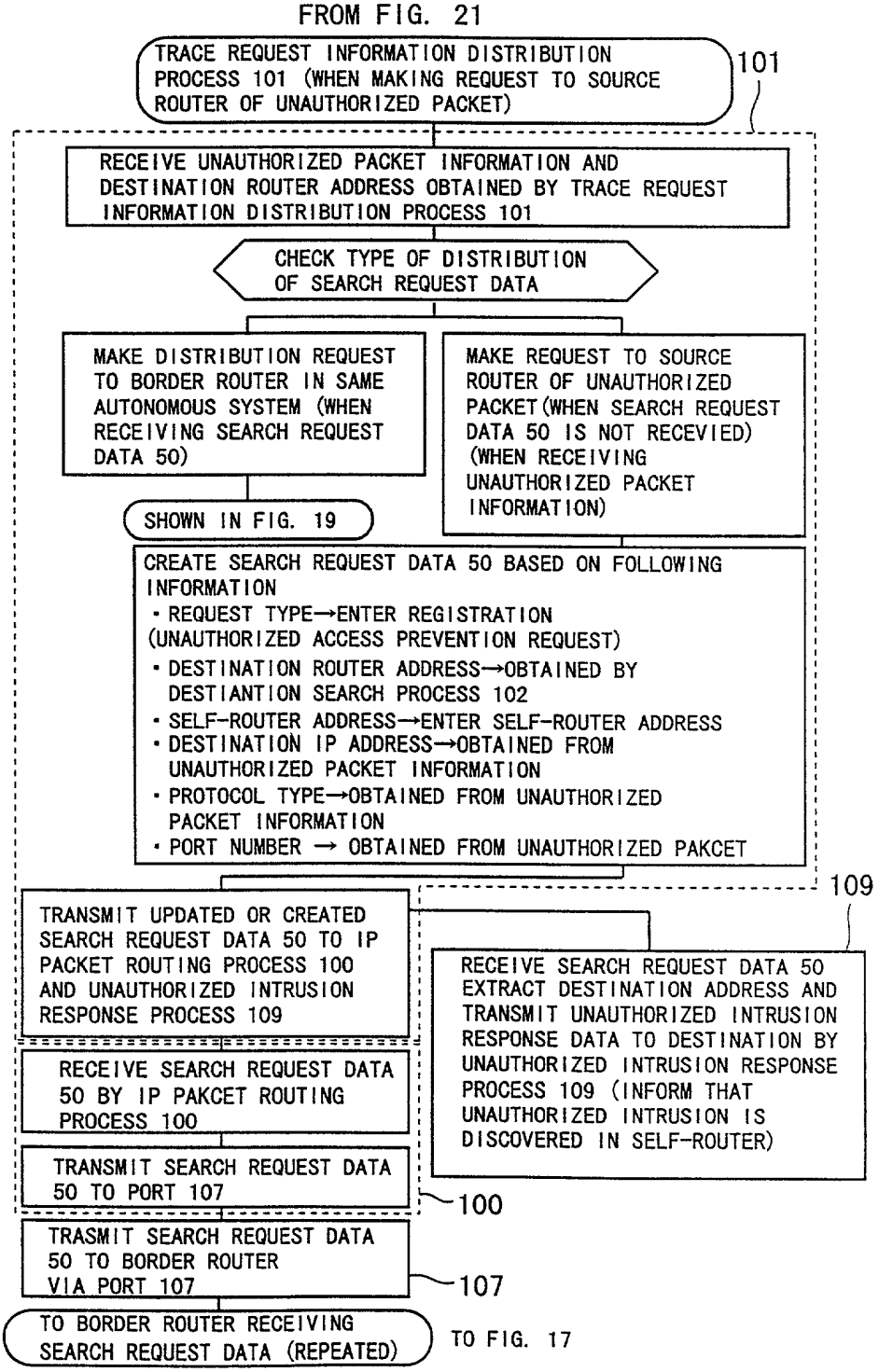
FIG. 21

FROM FIG. 20



TO FIG. 22

FIG. 22


FROM FIG. 21
TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101 (WHEN MAKING REQUEST TO SOURCE ROUTER OF UNAUTHORIZED PACKET)
101
RECEIVE UNAUTHORIZED PACKET INFORMATION AND DESTINATION ROUTER ADDRESS OBTAINED BY TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101
CHECK TYPE OF DISTRIBUTION OF SEARCH REQUEST DATA
MAKE DISTRIBUTION REQUEST TO BORDER ROUTER IN SAME AUTONOMOUS SYSTEM (WHEN RECEIVING SEARCH REQUEST DATA 50)
MAKE REQUEST TO SOURCE ROUTER OF UNAUTHORIZED PACKET (WHEN SEARCH REQUEST DATA 50 IS NOT RECEVIED) (WHEN RECEIVING UNAUTHORIZED PACKET INFORMATION)
SHOWN IN FIG. 19
CREATE SEARCH REQUEST DATA 50 BASED ON FOLLOWING INFORMATION
• REQUEST TYPE→ENTER REGISTRATION (UNAUTHORIZED ACCESS PREVENTION REQUEST)
• DESTINATION ROUTER ADDRESS→OBTAINED BY DESTIANTION SEARCH PROCESS 102
• SELF-ROUTER ADDRESS→ENTER SELF-ROUTER ADDRESS
• DESTINATION IP ADDRESS→OBTAINED FROM UNAUTHORIZED PACKET INFORMATION
• PROTOCOL TYPE→OBTAINED FROM UNAUTHORIZED PACKET INFORMATION
• PORT NUMBER → OBTAINED FROM UNAUTHORIZED PAKCET
TRANSMIT UPDATED OR CREATED SEARCH REQUEST DATA 50 TO IP PACKET ROUTING PROCESS 100 AND UNAUTHORIZED INTRUSION RESPONSE PROCESS 109
109
RECEIVE SEARCH REQUEST DATA 50 EXTRACT DESTINATION ADDRESS AND TRANSMIT UNAUTHORIZED INTRUSION RESPONSE DATA TO DESTINATION BY UNAUTHORIZED INTRUSION RESPONSE PROCESS 109 (INFORM THAT UNAUTHORIZED INTRUSION IS DISCOVERED IN SELF-ROUTER)
RECEIVE SEARCH REQUEST DATA 50 BY IP PAKCET ROUTING PROCESS 100
TRANSMIT SEARCH REQUEST DATA 50 TO PORT 107
100
TRASMIT SEARCH REQUEST DATA 50 TO BORDER ROUTER VIA PORT 107
107
TO BORDER ROUTER RECEIVING SEARCH REQUEST DATA (REPEATED)
TO FIG. 17